

Binary sequences with three-valued cross correlations of different lengths

March 20, 2015

Jinquan Luo*

Abstract– In this paper, new pairs of binary sequences with three cross correlation values are presented. The cross correlation values are shown to be low. Finally we present some numerical results and some open problems.

Index terms– Binary sequence, Correlation distribution, Linearized polynomial, Rank

1 Introduction

Sequences with low cross correlations have wide applications in many different communication systems. Let $u = (u_t)_{t=0}^{n-1}$ and $v = (v_t)_{t=0}^{n-1}$ be two binary sequences with length n . The cross correlation function of u and v with shift τ is defined by

$$C_\tau(u, v) = \sum_{t=0}^{n-1} (-1)^{u_{t+\tau} + v_t}. \quad (1)$$

The multiset $\{C_\tau(u, v) \mid 0 \leq \tau \leq n-1\}$ is called cross correlation distribution of the sequences u and v . For several decades, sequences with low cross correlations have attracted special interests from different aspects. In many cases the sequence

The author is with School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, China 430079. This work is supported by NSFC under grant 11471008.

E-mail addresses: luojinquan@mail.ccnu.edu.cn

v is a decimated sequence of u with some decimation d , that is, $v_t = u_{(dt)}$ for $0 \leq t \leq n-1$ where the subscript (dt) takes on the smallest non-negative integer equalling dt module n . If d and n are coprime, then v will have the same length as u and both these two sequences are called m -sequences of length n . For cross correlation of two binary m -sequences, together with a survey on historical results, the readers are referred to

In general the decimation d may be not coprime to n . Then the length of v will become $n' = n/\gcd(n, d)$ which is a factor of n . In this case we can consider the cross correlation function of a and b in a similar way as (1). In , Ness and Hellesteth studied the cross correlation between a m -sequence (u_t) of length $2^m - 1$ and its decimated sequence $(v_t) = (v_{(dt)})$ of length $2^{m/2} - 1$ with $d = (2^{m/2} + 1)^2/3$ (here $m \equiv 2 \pmod{4}$). Later, the result is generalized to the case $d = (2^{(m+2)/4} - 1)(2^{m/2} + 1)$ (see). In , they propose a conjecture that all three-valued cross correlation between two m -sequences of lengths $2^m - 1$ and $2^{m/2} - 1$ are characterized.

In this paper we will consider the cross correlation between two m -sequences of length $2^m - 1$ and $3(2^{m/2} - 1)$ with $m \equiv 2 \pmod{4}$. The cross correlation is proven to be three-valued. Our result does not violate this conjecture since the second sequence has length $3(2^{m/2} - 1)$, not $2^{m/2} - 1$. Our result reveals that if the length of the second sequence b is more flexible, there maybe exist more sequences with three-valued cross correlation.

Precisely, let k, l be odd integers coprime to each other. Let $m = 2k$, $q = 2^m$ and g be a primitive element of $\text{GF}(q)$. We will study cross correlation of sequences

$$u = (\text{Tr}_m(g^t))_{t=0}^{q-2} \quad (2)$$

and its decimated sequence

$$v = (\text{Tr}_m(g^{dt}))_{t=0}^{q-2} \quad (3)$$

with decimation $d = (2^{lk} + 1)/(2^l + 1)$. Then by (1), the cross correlation function with shift τ is

$$C_\tau(u, v) = \sum_{t=0}^{n-1} (-1)^{\text{Tr}_m(g^{t+\tau} + g^{dt})} = \sum_{x \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(x^d + ax)} \quad (4)$$

with $a = g^\tau$. Our main result is depicted in the sequel.

Theorem 1. *The cross correlation distribution $C_d(\tau)$ when τ runs from 0 to $q-2$ is as follows.*

values	frequencies	
-1	$\frac{(2^k+1)(7 \cdot 2^k+8)}{9}$	
$-1 + 2^{k+1}$	$\frac{(2^k+1)^2}{9}$	
$-1 - 2^{k+1}$	$\frac{(2^k+1)(2^k-2)}{9}$	\square

This paper is organized as follows. In Section II we will present some preliminaries which is needed to study the sequences, and also we will develop connections among the cross correlation function and two kinds of exponential sums $T(a, b)$ and $S(a, b)$. In Section III we will study $T(a, b)$ which is a kind of exponential sums from binary quadratic forms. In Section IV we will prove our main result. Finally in Section V we make some conclusions and also some open problems will be proposed.

2 Preliminaries

The following notations are fixed through the rest of the paper except for specific statements.

- Let k and l be two odd integers with $0 < l < k$ and $\gcd(l, k) = 1$. Let $d = \frac{2^{lk}+1}{2^{l+1}}$.
- Let $m = 2k$, $q = 2^m$. For positive integer i , let $\text{GF}(2^i)$ be the finite field with cardinality 2^i .
- Let g be a fixed primitive element of $\text{GF}(q)$ and $r = g^{2^k-1}$.
- For $j|i$, let $\text{Tr}_{i/j} : \text{GF}(2^i) \rightarrow \text{GF}(2^j)$ be the trace mapping defined by $\text{Tr}_{i/j}(x) = x + x^{2^j} + x^{2^{2j}} + \cdots + x^{2^{i-j}}$. In particular, we use the notation Tr_i to replace $\text{Tr}_{i/1}$ for abbreviation.

If we regard $\text{GF}(q)$ as a vector space over $\text{GF}(2)$ with dimension m , then $Q(x) = \text{Tr}_m \left(\sum_i a_i x^{p^i+1} \right)$ is a binary quadratic form of m variables. It is well-known that $Q(x)$ is equivalent to one of the following three standard forms (see [15], Theorem):

(Type I): $x_1x_2 + x_3x_4 + \cdots + x_{2v-1}x_{2v}$;

(Type II): $x_1x_2 + x_3x_4 + \cdots + x_{2v-1}x_{2v} + x_{2v+1}^2$;

(Type III): $x_1x_2 + x_3x_4 + \cdots + x_{2v-1}x_{2v} + x_{2v-1}^2 + x_{2v}^2$

where $2v$ is codimension of $\text{GF}(2)$ -vector space V_m which is defined by

$$V_m = \{x \in \text{GF}(q) \mid Q(x+y) + Q(x) + Q(y) = 0 \text{ for all } y \in \text{GF}(q)\}.$$

Then $\sum_{x \in \text{GF}(2)^m} (-1)^{Q(x)}$ can be evaluated if we know which standard form $Q(x)$ lies in.

Lemma 1.

$$\sum_{x \in \text{GF}(2)^m} (-1)^{Q(x)} = \begin{cases} 2^{m-v}, & \text{if } Q(x) \text{ belongs to Type I;} \\ 0, & \text{if } Q(x) \text{ belongs to Type II;} \\ -2^{m-v}, & \text{if } Q(x) \text{ belongs to Type III.} \end{cases}$$

Proof. If $Q(x)$ belongs to Type I, then

$$\sum_{x \in \text{GF}(2)^m} (-1)^{Q(x)} = 2^{m-2v} \prod_{i=1}^v \sum_{x_{2i-1}, x_{2i}=0}^1 (-1)^{x_{2i-1}x_{2i}} = 2^{m-2v} \cdot 2^v = 2^{m-v}.$$

If $Q(x)$ belongs to Type II, then

$$\sum_{x \in \text{GF}(2)^m} (-1)^{Q(x)} = 2^{m-2v-1} \prod_{i=1}^v \sum_{x_{2i-1}, x_{2i}=0}^1 (-1)^{x_{2i-1}x_{2i}} \sum_{x_{2v+1}=0}^1 (-1)^{x_{2v+1}^2} = 0$$

since the last summation equals to zero.

If $Q(x)$ belongs to Type III, then

$$\sum_{x \in \text{GF}(2)^m} (-1)^{Q(x)} = 2^{m-2v} \prod_{i=1}^{v-1} \sum_{x_{2i-1}, x_{2i}=0}^1 (-1)^{x_{2i-1}x_{2i}} \sum_{x_{2v-1}, x_{2v}=0}^1 (-1)^{x_{2v-1}x_{2v} + x_{2v-1}^2 + x_{2v}^2} = -2^{m-v}$$

since the last summation equals to -1 . □

Recall that $r = g^{2^k-1}$ and define $\delta = r^d$.

Lemma 2. The element δ is primitive in $\text{GF}(4)$, that is, $\delta^2 = \delta + 1 = \delta^{-1}$.

Proof. We can calculate $\delta^{2^l+1} = g^{(2^k-1)(2^l+1)} = g^{(2^{2k}-1)\frac{2^l+1}{2^k+1}} = 1$. By $\gcd(2^l+1, 2^{2k}-1) = 3$ we can deduce $\delta^3 = 1$.

It remains to show that $\delta \neq 1$. Otherwise, by $\delta = g^{(2^k-1)\frac{2^l+1}{2^l+1}} = 1$ we have

$$2^{2k} - 1 \mid (2^k - 1) \frac{2^{lk} + 1}{2^l + 1}$$

which implies

$$2^k + 1 \mid \frac{2^{lk} + 1}{2^l + 1}.$$

So we can deduce

$$(2^k + 1)(2^l + 1) \mid 2^{lk} + 1. \quad (5)$$

Denote by $v_3(n)$ the highest power of 3 dividing n , that is, $n = 3^{v_3(n)}n'$ with n' coprime to 3. For n coprime to 3, define

$$\text{ord}_n(a) = \min\{s > 0 \mid a^s \equiv 1 \pmod{n}\}.$$

Then $\text{ord}_9(2) = 6$.

Then for odd f , we have $v_3(2^f + 1) \geq 1$ and then

$$\begin{aligned} v_3(2^{3f} + 1) &= v_3((2^f + 1)(2^{2f} - 2^f + 1)) \\ &= v_3(2^f + 1) + v_3((2^f + 1)^2 - 3 \cdot 2^f) = v_3(2^f + 1) + 1 \end{aligned}$$

where the last equality from $v_3((2^f + 1)^2) \geq 2$ and $v_3(3 \cdot 2^f) = 1$. Then by induction we obtain

$$v_3(2^f + 1) = v_3(2^{3^{v_3(f)}f'} + 1) = v_3(f) + v_3(2^{f'} + 1). \quad (6)$$

Since odd f' is not divisible by 3, then we can deduce $2^{f'} + 1 \not\equiv 0 \pmod{9}$. Otherwise $2^{2f'} \equiv 1 \pmod{9}$ which implies $6 \mid 2f'$ and $3 \mid f'$. It is a contradiction. Therefore $v_3(2^{f'} + 1) = 1$ and then by (6) we have $v_3(2^f + 1) = v_3(f) + 1$. Then by (5) we obtain $v_3((2^k + 1)(2^l + 1)) = 1 + v_3(k) + 1 + v_3(l) \leq v_3(2^{lk} + 1) = 1 + v_3(lk) = 1 + v_3(l) + v_3(k)$ which leads to a contradiction.

As a result, we can deduce $\delta \in \text{GF}(4) \setminus \{0, 1\}$ and then the result follows. \square

By (4) we obtain that

$$C_\tau(u, v) = S(a) - 1 \quad (7)$$

with $a = g^\tau \in \text{GF}(q)^*$ and

$$S(a) = \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d + ax)}. \quad (8)$$

Then we turn to study the binary exponential sum $S(a)$. Firstly we observe that $\gcd(2^l + 1, 2^m - 1) = 3$ and $(2^l + 1)d = 2^{lk} + 1 \equiv 2^k + 1 \pmod{2^m - 1}$. Since $r = g^{2^k - 1}$ is a noncube in $\text{GF}(q)$, then images of the mappings $x \mapsto x^{2^l + 1}$, $x \mapsto rx^{2^l + 1}$ and $x \mapsto r^{-1}x^{2^l + 1}$ (all the three maps are from $\text{GF}(q)$ to $\text{GF}(q)$) covers each element of $\text{GF}(q)$ exactly three times when x runs through $\text{GF}(q)$. Therefore

$$\begin{aligned} 3S(a) = & \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^{2^k+1} + ax^{2^l+1})} + \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(\delta x^{2^k+1} + rax^{2^l+1})} \\ & + \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(\delta^{-1}x^{2^k+1} + r^{-1}ax^{2^l+1})} \end{aligned} \quad (9)$$

where $\delta = r^d$.

We observe that $x^{2^k+1} \in \text{GF}(2^k)$ and $\delta + \delta^{2^k} = 1$. Hence $\text{Tr}_m(x^{2^k+1}) = 0$ and $\text{Tr}_m(\delta x^{2^k+1}) = \text{Tr}_k((\delta + \delta^{2^k})x^{2^k+1}) = \text{Tr}_k(x^{2^k+1})$. In the same way $\text{Tr}_m(\delta^{-1}x^{2^k+1}) = \text{Tr}_k(x^{2^k+1})$. It follows from (9) that

$$3S(a) = T(a, 0) + T(ra, \delta) + T(r^{-1}a, \delta) \quad (10)$$

where

$$T(a, b) = \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(ax^{2^l+1} + bx^{2^k+1})}. \quad (11)$$

In order to evaluate $T(a, b)$, it is sufficient to study quadratic form

$$Q_{a,b}(x) := \text{Tr}_m(ax^{2^l+1} + bx^{2^k+1}). \quad (12)$$

Define

$$L_{a,b}(x) = a^{2^{2k-2l}} x^{2^{2k-2l}} + (b^{2^{2k-l}} + b^{2^{k-l}}) x^{2^{k-l}} + a^{2^{k-l}} x \quad (13)$$

and

$$V_m(a, b) = \{x \in \text{GF}(q) \mid Q_{a,b}(x+y) + Q_{a,b}(x) + Q_{a,b}(y) = 0 \text{ for all } y \in \text{GF}(q)\}. \quad (14)$$

Now we turn to study $V_m(a, b)$ which can be formulated as follows.

$$\begin{aligned}
\dim_{\text{GF}(2)} V_m(a, b) = m - 2v &\iff \text{for all } y \in \text{GF}(q), Q_{a,b}(x+y) + Q_{a,b}(x) + Q_{a,b}(y) = 0 \\
&\quad \text{has } 2^{m-2v} \text{ common solutions } x \in \text{GF}(q) \\
&\iff \text{for all } y \in \text{GF}(q), \text{Tr}_m(ax^{2^l}y + ax^2y^{2^l} + bx^{2^k}y + bxy^{2^k}) = 0 \text{ has } 2^{m-2r} \\
&\quad \text{common solutions } x \in \text{GF}(q) \\
&\iff \text{for all } y \in \text{GF}(q), \text{Tr}_m\left(y^{2^{2k-l}}(a^{2^{k-l}}x + a^{2^{2k-2l}}x^{2^{2k-2l}} + (b^{2^{2k-l}} + b^{2^{k-l}})x^{2^{k-l}})\right) = 0 \\
&\quad \text{has } 2^{m-2v} \text{ common solutions } x \in \text{GF}(q) \\
&\iff L_{a,b}(x) = a^{2^{2k-2l}}x^{2^{2k-2l}} + (b^{2^{2k-l}} + b^{2^{k-l}})x^{2^{k-l}} + a^{2^{k-l}}x = 0 \\
&\quad \text{has } 2^{m-2v} \text{ solutions } x \in \text{GF}(q).
\end{aligned}$$

Therefore

$$V_m(a, b) = \{x \in \text{GF}(q) \mid L_{a,b}(x) = 0\}.$$

Note that $\gcd(k-l, m) = 2$ and $V_m(a, b)$ is also a $\text{GF}(2^m) \cap \text{GF}(2^e) = \text{GF}(4)$ -linear space. Then we can determine the possible dimensions of $V_m(a, b)$.

Lemma 3. For any $a \in \text{GF}(q)^*$, the dimension of $\text{GF}(4)$ -linear space $V_m(a, b)$ is at most 2.

Proof. Fix an algebraic closure $\text{GF}(2^\infty)$ of $\text{GF}(2)$, since the degree of $\text{GF}(4)$ -linearized polynomial $L_{a,b}(x)$ is 2^{2e} and $L_{a,b}(x) = 0$ has no multiple roots in $\text{GF}(2^\infty)$, then the zeroes of $L_{a,b}(x)$ in $\text{GF}(2^\infty)$, say $V_\infty(a, b)$, form an $\text{GF}(2^e)$ -vector space of dimension 2. Note that $\gcd(e, m) = 2$. Then $V_m(a, b) = V_\infty(a, b) \cap \text{GF}(2^m)$ is a vector space on $\text{GF}(2^{\gcd(e, m)}) = \text{GF}(4)$ with dimension at most 2 since any elements in $\text{GF}(2^m)$ which are linear independent over $\text{GF}(4)$ are also linear independent over $\text{GF}(2^e)$. \square

The following binary exponential sum will be useful(see [15], [16]).

Lemma 4. For $h \mid 2^k + 1$, we have

$$\sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(ax^h)} = \begin{cases} (h-1)2^k, & \text{if } a = g^{hi} \text{ for some } i, \\ -2^k, & \text{otherwise.} \end{cases} \quad \square$$

Now we introduce some moment identities to determine the occurrences of all possible values of $S(a)$.

Lemma 5. For $S(a)$ defined in (8), we have

- (i). $\sum_{a \in \text{GF}(q)^*} S(a) = \frac{2^k+1}{3} \cdot 2^{k+1}.$
- (ii). $\sum_{a \in \text{GF}(q)^*} S(a)^2 = \frac{2^{2k+2}(2^k+1)(2^{k+1}-1)}{9}.$

Proof. (i). We calculate

$$\begin{aligned} \sum_{a \in \text{GF}(q)^*} S(a) &= \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d)} \sum_{a \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(ax)} \\ &= 2^{2k} - 1 - \sum_{x \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(x^d)} \\ &= 2^{2k} - 1 - \left(\left(\frac{2^k+1}{3} - 1 \right) 2^k - 1 \right) = \frac{2^k+1}{3} \cdot 2^{k+1}. \end{aligned}$$

(ii). We obtain

$$\begin{aligned} \sum_{a \in \text{GF}(q)^*} S(a)^2 &= \sum_{x, y \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d+y^d)} \sum_{a \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(a(x+y))} \\ &= (2^{2k} - 1) \sum_{x=y} (-1)^{\text{Tr}_m(x^d+y^d)} - \sum_{x \neq y} (-1)^{\text{Tr}_m(x^d+y^d)}. \end{aligned}$$

Denote by $A = \sum_{x=y} (-1)^{\text{Tr}_m(x^d+y^d)}$ and $B = \sum_{x \neq y} (-1)^{\text{Tr}_m(x^d+y^d)}$. Then $A = 2^{2k}$ and

$$A + B = \sum_{x, y} (-1)^{\text{Tr}_m(x^d+y^d)} = \left(\sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d)} \right)^2 = \frac{2^{2k}(2^k-2)^2}{9}.$$

Therefore $B = 2^{2k}(2^k-5)(2^k+1)/9$ and

$$\sum_{a \in \text{GF}(q)^*} S(a)^2 = 2^{2k} (2^{2k} - 1) - \frac{2^{2k}(2^k-5)(2^k+1)}{9} = \frac{2^{2k+2}(2^k+1)(2^{k+1}-1)}{9}.$$

□

3 On binary exponential sum $T(a, b)$

For any $x \in \text{GF}(q)^*$ and $0 \leq i \leq 2$, it is easy to see $(\delta^i x)^{2^l+1} = x^{2^l+1}$ and $(\delta^i x)^{2^k+1} = x^{2^k+1}$. Hence

$$\text{Tr}_m \left(a(\delta^i x)^{2^l+1} + b(\delta^i x)^{2^k+1} \right) = \text{Tr}_m \left(ax^{2^l+1} + bx^{2^k+1} \right).$$

As a consequence,

Lemma 6. For any $a, b \in \text{GF}(q)$, we have $T(a, b) \equiv 1 \pmod{3}$.

Proof. Let D be a set of coset representatives of $\text{GF}(q)^*/\text{GF}(4)^*$. Then

$$\begin{aligned} T(a, b) &= 1 + \sum_{x \in D} \sum_{i=0}^2 (-1)^{\text{Tr}_m(a(\delta^i x)^{2^l+1} + b(\delta^i x)^{2^k+1})} \\ &= 1 + 3 \cdot \sum_{x \in D} (-1)^{\text{Tr}_m(ax^{2^l+1} + bx^{2^k+1})} \equiv 1 \pmod{3}. \end{aligned}$$

□

Now we can decide the possible values of $T(a, b)$.

Lemma 7. The exponential sum

$$T(a, b) = \begin{cases} -2^k, & \text{if } \dim_{\text{GF}(4)} V_m(a, b) = 0, \\ 2^{k+1}, & \text{if } \dim_{\text{GF}(4)} V_m(a, b) = 1, \\ -2^{k+2}, & \text{if } \dim_{\text{GF}(4)} V_m(a, b) = 2. \end{cases}$$

Proof. If $\dim_{\text{GF}(4)} V_m(a, b) = 0$, then $m - 2v = 0$ and $v = k$. Hence by Lemma 1 we obtain $T(a, b) = \pm 2^k$. Combining Lemma 6 we can deduce $T(a, b) = -2^k$.

If $\dim_{\text{GF}(4)} V_m(a, b) = 1$, then $\dim_{\text{GF}(2)} V_m(a, b) = 2$ and $m - 2v = 2$ which yields $v = k - 1$. Hence by Lemma 1 we obtain $T(a, b) = \pm 2^{k+1}$ or 0. Combining Lemma 6 we obtain $T(a, b) = 2^{k+1}$.

Similarly, if $\dim_{\text{GF}(4)} V_m(a, b) = 2$, then $T(a, b) = -2^{k+2}$. □

To evaluate $S(a)$, we need to deal with $T(a, 0)$, $T(ra, \delta)$ and $T(r^{-1}a, \delta^{-1})$ simultaneously.

Lemma 8. For $a \in \text{GF}(q)^*$, we have

$$T(a, 0) = \begin{cases} 2^{k+1}, & \text{if } a \text{ is a cubic,} \\ -2^k, & \text{if } a \text{ is not a cubic.} \end{cases}$$

Proof. In this case, $L_{a,0}(x) = a^{2^{2e}} x^{2^{2e}} + a^{2^{k+e}} x = 0$ has nonzero solution in $\text{GF}(q)$ if and only if

$$x^{2^{2e}-1} = \left(a^{2^l-1}\right)^{2^{2e}}.$$

Since $\gcd(2^{2e} - 1, q - 1) = 3$ and $\gcd(2^l - 1, q - 1) = 1$, this equation has nonzero solution if and only if a is a cubic in $\text{GF}(q)^*$. In this case, it has exactly three nonzero solutions. Taking the solution $x = 0$ into account, we obtain that $L_{a,0}(x) = 0$ has four or one solutions in $\text{GF}(q)$ depending on a in cubic in $\text{GF}(q)^*$ or not. Therefore the result follows from Lemma 7. □

Lemma 9. If a is a nonzero cubic in $\text{GF}(q)^*$, then

$$T(ra, \delta) = T(r^{-1}a, \delta^{-1}) = -2^k \text{ or } 2^{k+1}.$$

Proof. Firstly we show that $T(ra, \delta) = T(r^{-1}a, \delta^{-1})$. Note that $\delta^{2^k} = \delta^2 = \delta^{-1}$ and $\delta + \delta^2 = 1$. We can reformulate

$$T(ra, \delta) = \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(rx^{2^l+1}) + \text{Tr}_k(x^{2^k+1})}$$

and

$$T(r^{-1}a, \delta) = \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(r^{-1}ax^{2^l+1}) + \text{Tr}_k(x^{2^k+1})}.$$

Since a is a nonzero cubic in $\text{GF}(q)$, we assume $a = g^{3s}$ for some integer s . It is easy to see that $\gcd((2^k - 1)(2^l + 1), 2^k + 1) = 3$. Hence there exists integers i and j satisfying

$$(2^k - 1)(2^l + 1)i + (2^k + 1)j = 3s.$$

By substituting $x = g^{-(2^k-1)i}y$, we obtain $ax^{2^l+1} = g^{3s-(2^k-1)(2^l+1)i}y^{2^l+1} = g^{(2^k+1)j}y^{2^l+1}$ and $x^{2^k+1} = y^{2^k+1}$. Denote by $b = g^{(2^k+1)j} \in \text{GF}(2^k)^*$. Then $T(ra, \delta) = T(rb, \delta)$ and $T(r^{-1}a, \delta) = T(r^{-1}b, \delta)$. Moreover

$$\begin{aligned} T(rb, \delta) &= \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m((rbx^{2^l+1})^{2^k}) + \text{Tr}_k(x^{2^k+1})} \\ &= \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(r^{-1}bx^{2^k(2^l+1)}) + \text{Tr}_k(x^{2^k+1})} = T(r^{-1}b, \delta). \end{aligned}$$

Therefore $T(ra, \delta) = T(rb, \delta) = T(r^{-1}b, \delta) = T(r^{-1}a, \delta)$. From now on we may assume $a \in \text{GF}(2^k)$.

Secondly we show that $T(ra, \delta) \neq -2^{k+2}$ which is equivalent to saying that $\dim_{\text{GF}(4)} V_{ra, \delta} \neq 2$. Assume, on the contrary, that $\dim_{\text{GF}(4)} V_{ra, \delta} = 2$. Then there exists x_1, x_2 with $x_1 \neq x_2, \delta x_2, \delta^2 x_2$. Thereafter

$$(ra)^{2^{2e}} x_1^{2^{2e}} + x_1^{2^e} + (ra)^{2^{k+e}} x_1 = (ra)^{2^{2e}} x_2^{2^{2e}} + x_2^{2^e} + (ra)^{2^{k+e}} x_2 = 0$$

which yields

$$\left((ra)^{2^{2e}} x_1^{2^{2e}} + (ra)^{2^{k+e}} x_1 \right) x_2^{2^e} = \left((ra)^{2^{2e}} x_2^{2^{2e}} + (ra)^{2^{k+e}} x_2 \right) x_1^{2^e}.$$

A routine calculation implies that

$$a^{2^e(2^e-1)} (x_1^{2^e} x_2 + x_1 x_2^{2^e})^{1-2^e} = r^{2^e(2^e+1)}.$$

The left hand side is a cubic in $\text{GF}(q)$. But the right hand side is not since $r = g^{2^k-1}$ and $3 \nmid \gcd((2^k-1)(2^e+1), q-1) = 2^k-1$. It leads to a contradiction. \square

In the sequel we will consider $T(ra, \delta)$ and $T(r^{-1}a, \delta)$ in the case a is noncubic.

Lemma 10. If a is a noncubic, then at least one of $T(ra, \delta)$ and $T(r^{-1}a, \delta)$ is equal to -2^k .

Proof. It suffices to show that at least one of $L_{ra, \delta}(x) = 0$ and $L_{r^{-1}a, \delta}(x) = 0$ has only one solution $x = 0$ in $\text{GF}(q)$. Indeed, assume there exist $x_1, x_2 \in \text{GF}(q)^*$ such that

$$(ra)^{2^{2e}} x_1^{2^{2e}} + x_1^{2^e} + (ra)^{2^{k+e}} x_1 = (r^{-1}a)^{2^{2e}} x_2^{2^{2e}} + x_2^{2^e} + (r^{-1}a)^{2^{k+e}} x_2 = 0$$

which implies that

$$\left((ra)^{2^{2e}} x_1^{2^{2e}} + (ra)^{2^{k+e}} x_1 \right) x_2^e = \left((r^{-1}a)^{2^{2e}} x_2^{2^{2e}} + (r^{-1}a)^{2^{k+e}} x_2 \right) x_1^e.$$

It can be transformed to

$$\left(r^{-2^e} x_1^{2^e} x_2 + r^{2^e} x_1 x_2^{2^e} \right)^{2^e-1} = a^{2^{2e}(2^l-1)}.$$

Note that $\gcd(2^e-1, q-1) = 3$ and $\gcd(2^l-1, q-1) = 1$. Then a must be a cubic which is a contradiction. \square

4 Proof of main result

Now we are ready to give all the possible values of $S(a)$ for $a \in \text{GF}(q)^*$.

Lemma 11. For $a \in \text{GF}(q)^*$, the possible values of $S(a)$ are $0, 2^{k+1}, -2^{k+1}$ and -2^k . Precisely,

- Case I: if a is nonzero cubic, then $S(a) = 0$ or 2^{k+1} ;
- Case II: if a is noncubic, then $S(a) = 0, -2^k$ or -2^{k+1} .

Proof. If a is a nonzero cubic, then $T(a) = 2^{k+1}$. From Lemma 9 we have $T(ra, \delta) = T(r^{-1}a, \delta) = -2^k$ or 2^{k+1} . As a consequence, $S(a) = (2^{k+1} - 2^k - 2^k)/3 = 0$ or $S(a) = (2^{k+1} + 2^{k+1} + 2^{k+1})/3 = 2^{k+1}$.

If a is a noncubic, then $T(a) = -2^k$. By Lemma 10 we obtain $S(a) = (-2^k - 2^k - 2^k)/3 = -2^k$ or $S(a) = (-2^k - 2^k + 2^{k+1})/3 = 0$ or $S(a) = (-2^k - 2^k - 2^{k+2})/3 = -2^{k+1}$. \square

When a runs through $\text{GF}(q)^*$, suppose $S(a)$ takes on the value zero N_0 times, -2^k is taken on N_1 times, 2^{k+1} is taken on N_2 times and -2^{k+1} is taken on N_3 times. Since 2^{k+1} only occurs in Case I (see Lemma 11), then N_2 can be calculated directly.

Lemma 12.

$$N_2 = \frac{(2^k + 1)^2}{9}.$$

Proof.

$$\begin{aligned} 2^{k+1}N_2 &= \sum_{a \text{ nonzero cubic}} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d + ax)} \\ &= \frac{1}{3} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}_m(x^d)} \sum_{b \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(b^3x)} \\ &= \frac{1}{3} \left((q - 1 + (2^{k+1} - 1)) \sum_{x \text{ nonzero cubic}} (-1)^{\text{Tr}_m(x^d)} + (-2^k - 1) \sum_{x \text{ non cubic}} (-1)^{\text{Tr}_m(x^d)} \right) \\ &= \frac{1}{3} (q - 1 + (2^{k+1} - 1) \cdot A + (-2^k - 1) \cdot B) \end{aligned} \tag{15}$$

where $A = \sum_{x \text{ nonzero cubic}} (-1)^{\text{Tr}_m(x^d)}$ and $B = \sum_{x \text{ non cubic}} (-1)^{\text{Tr}_m(x^d)}$.

Since when x runs through $\text{GF}(q)^*$, x^{2^l+1} runs through each nonzero cubic in $\text{GF}(q)$ exactly three times, then we can calculate

$$A = \frac{1}{3} \sum_{y \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(y^{2^k+1})} = \frac{q-1}{3}$$

and

$$A + B = \sum_{x \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(x^d)} = \sum_{x \in \text{GF}(q)^*} (-1)^{\text{Tr}_m(x^{(2^k+1)/3})} = 2^k(2^k - 2)/3 - 1.$$

Substituting A and B into (15), we obtain

$$N_2 = \frac{(2^k + 1)^2}{9}. \quad (16)$$

□

Now we are ready to determine the cross correlation of the sequences u defined in (2) and v defined in (3).

Proof of Theorem 1: Recall the definitions of N_i ($0 \leq i \leq 2$) and the value of N_2 in (16). Then we have

$$N_0 + N_1 + N_3 = 2^{2k} - 1 - N_2 = \frac{(2^k + 1)(2^{k+3} - 10)}{9}. \quad (17)$$

From Lemma 5 we obtain

$$N_1 + 2N_3 = \frac{2(2^k + 1)(2^k - 2)}{9} \quad (18)$$

$$N_1 + 4N_3 = \frac{4(2^k + 1)(2^k - 2)}{9}. \quad (19)$$

Solving the system equations consisting of (17)-(19), we can calculate

$$N_0 = \frac{(2^k + 1)(7 \cdot 2^k + 8)}{9}, \quad N_1 = 0, \quad N_3 = \frac{(2^k + 1)(2^k - 2)}{9}. \quad \square$$

Combing Lemma (16) we complete the proof of Theorem 1.

5 Conclusion

In this paper, we studied the cross correlation between one m -sequence of length $2^{2k} - 1$ and its decimated sequence of length $3(2^k - 1)$. The cross correlation has three possible values: 0, 2^{k+1} , -2^{k+1} . Moreover, the cross correlation distribution is also determined.

References

- [1] H. Dobbertin, P. Felke, T. Hellesteth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums", *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006.

- [2] C. Ding and X. Tang, “The cross correlation of binary sequences with optimal autocorrelation”, *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1694–1701, April 2010.
- [3] T. Helleseeth, “Some results about the cross-correlation function between two maximal-linear sequences,” *Discrete Math.*, vol. 16, pp. 209–232, 1976.
- [4] T. Helleseeth and P.V. Kumar, “Sequences with low correlation”, in *Handbook of Coding Theory*, chap. 21, V.Pless and W.Huffman Eds., Amsterdam, The Netherlands, Elsevier, 1998.
- [5] A. Johansen and T. Helleseeth, “A family of m -sequences with five valued cross correlation”, *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 880–889, Feb.2009.
- [6] A. Johansen, T. Helleseeth and A. Kholosha, “Further results on m -sequences with five valued cross correlation”, *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5792–5802, Dec.2009.
- [7] X. Liu, M. Harrison and Y. Luo, “A note on the five valued conjectures of Johansen, Helleseeth and Kholosha and zeta function”, *IEEE Comm. Letters*, vol. 18, no. 9, pp. 1483–1486, Sept. 2014.
- [8] T. Niho, “Multi-valued cross-correlation functions between two maximal linear recursive sequences,” Ph.D dissertation, Univ. Southern California, Los Angeles, 1976.
- [9] G.J. Ness and T. Helleseeth, “A new family of four-valued cross correlation between m -sequences of different lengths”, *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4308–4313, Nov. 2007.
- [10] K. Ranto and P. Rosendahl, “On four-valued cross correlation functions of m -sequences”, *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5533–5536, Dec. 2006.
- [11] G.J. Ness and T. Helleseeth, “Cross correlation of m -sequences with different lengths”, *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1637–1648, April 2006.
- [12] G.J. Ness and T. Helleseeth, “A new three-valued cross correlation between m -sequences of different lengths”, *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4695–4701, Oct. 2006.

- [13] G.J. Ness and T. Helleseeth, “Characterization of m -sequences of length $2^{2k} - 1$ and $2^k - 1$ with three-valued cross correlation”, *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2236–2245, June 2007.
- [14] T. Zhang, S. Li, T. Feng, and G. Ge, “Some new results on the cross correlation of m -sequences,” *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 3062–3068, May 2014.
- [15] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics, vol. 20, Cambridge University Press, Cambridge, 1983.
- [16] M. Moio, A note on evaluations of some exponential sums, *Acta Arithmetica*, vol. 93, pp. 117–119, 2000.
- [17] T. Helleseeth, L. Hu, A. Kholosha, X. Zeng, N. Li, W. Jiang, “Period-different m -sequences with at most four-valued cross correlation”, *IEEE Trans. Inf. Theory* vol. 55, no. 7, pp. 3305–3311, July 2009.